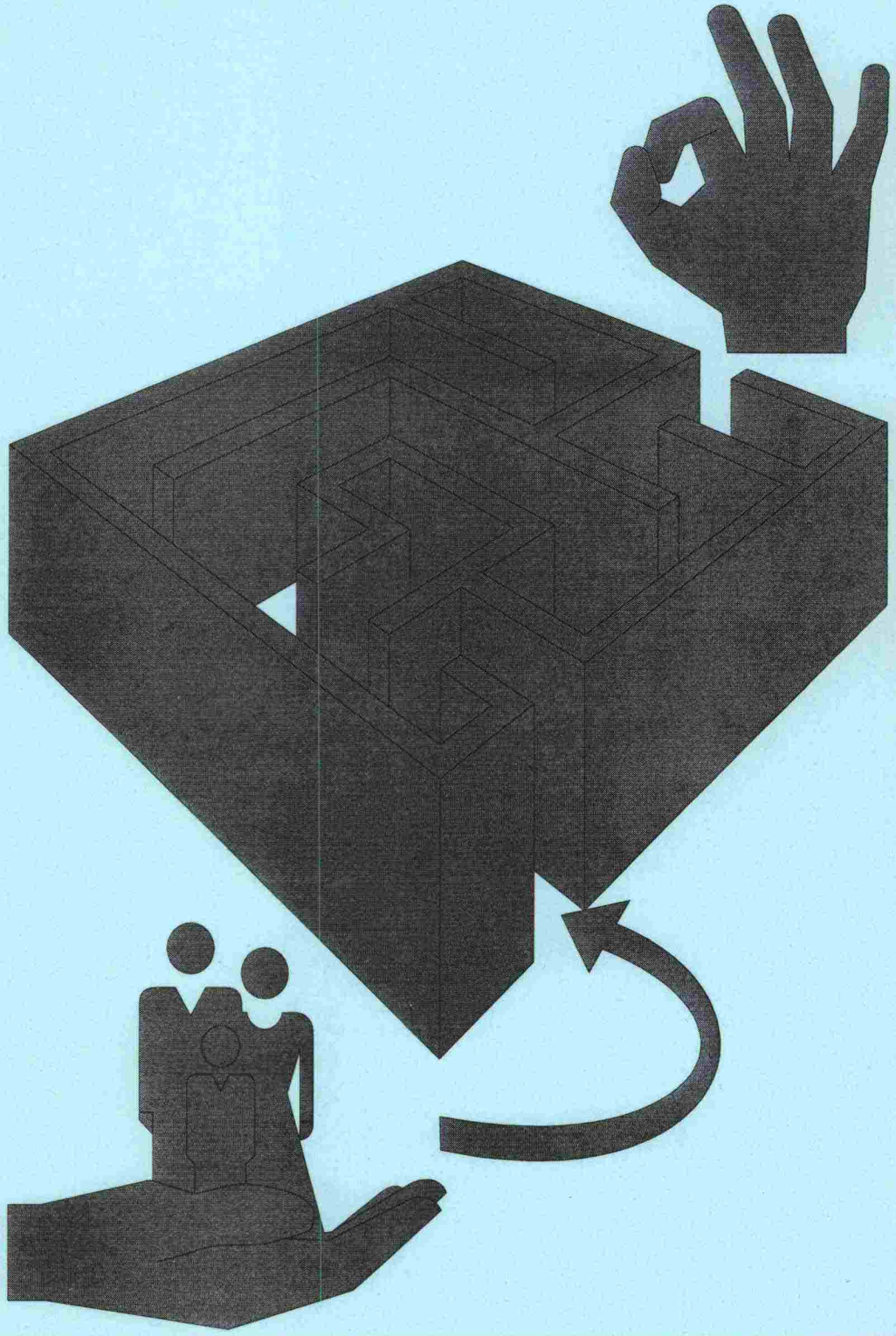
Tielaitos

Kaakkois-Suomen tiepiirin turvallisuusohje



10/1994

Kouvola 1994

Kaakkois-Suomen tiepiiri

Kaakkois-Suomen tiepiirin toimintaa ohjaava julkaisu 10/1994

Kaakkois-Suomen tiepiirin turvallisuusohje

Tielaitos
Kaakkois-Suomen tiepiiri

Kouvola 1994

TIEL KaS 10/94
Kaakkois-Suomen tiepiiri
Kouvola

Kansikuva ja taitto: Pirkko Heino

Tielaitos
Kaakkois-Suomen tiepiiri
Kauppamiehenkatu 4
PL 13
45101 KOUVOLA
Puh. vaihde (951) 7761

Tielaitos
Kaakkois-Suomen tiepiiri

OHJE

60/95/03/KAS

13.01.1995

58/95

Kaakkois-Suomen tiepiirin yksiköt

Säädösperusta

Korvaa/muuttaa

Kohderyhmät
KAAKKOIS-SUOMEN TIEPIIRI

Voimassa
1.2.1995 - TOISTAISEKSI

Asiasanat
TURVALLISUUS, YRITYSTURVALLISUUS, RISKIEN HALLINTA

KAAKKOIS-SUOMEN TIEPIIRIN TURVALLISUUSOHJE

Erilaiset vahinkoriskit ovat lisääntyneet. Ne uhkaavat yhä useammin tiepiirin toimintaa ja sen jatkuvuutta. Tyypillisimmät riskit kohdistuvat omaisuuteen. Tietoturvallisuuteen liittyvät uhat ovat tulleet varteenotettaviksi atk-toiminnan yleistymisen ja siitä riippuvuuden lisääntymisen myötä. Liiketaloudellisetkin riskit tulevat kuvaan liikelaitostumisen myötä.

Turvallisuussuunnittelu muodostaa lähtökohdan turvallisuuden arvioinnille ja kehittämiselle työpaikoilla. Sen avulla tehdään paikalliset riskianalyysit ja työpaikan turvallisuussuunnitelma.

Turvallisuustoiminnan kehittäminen alkaa aina riskianalyysistä. Siinä tarkoitetaan kyseisen työpaikan riskit sekä niiden todennäköisyys ja suuruus.

Turvallisuusstrategian mukaan turvallisuutta parantavat toimet kohdistetaan niihin kohteisiin, joissa riskit ovat suurimmat. Toimintojen kustannukset mitoitetaan niin, että ne ovat pienemmät kuin vahingoista aiheutuvat kustannukset.

Yritysturvallisuus on tielaitoksen toiminnassa käsitteenä uusi. Sen osa-alueita ovat muun muassa toimitila-, henkilöstö-, toiminta-, tieto- ja ympäristöturvallisuus, pelastustoiminta, työsuojelu, varautuminen ja ulkomaantoimintojen turvallisuus sekä turvallisuus- ja riskihallinto. Yritysturvallisuudesta vastaa linjajohto.

Tiejohtaja

Ville Mäkelä

LISÄTIETOJA
KaS/Toimistopalvelut
Puh. (951) 7761

JAKELU/MYYNTI
KaS/Toimistopalvelut
Puh. (951) 7761

ALKUSANAT

Kaakkois-Suomen tiepiirin turvallisuusohje sisältää ohjeet työpaikkakohtaiselle turvallisuuden arvioinnille ja turvallisuussuunnitelman laatimiselle.

Ohjeen on laatinut työryhmä, jonka jäseninä olivat Raimo Loponen (pj.), Hannu Puustinen, Vesa Romppanen, Pentti Valjakka ja Heljä Vesalainen. Pirkko Heino on vastannut ohjeen ulkoasusta ja avustanut kielenhuollossa.

Työssä tarvittavaa tietoa on hankittu sekä piirin sisäisistä että ulkopuolisista lähteistä.

Lähtökohtana työlle on ollut erilaisten vahinkoriskien lisääntyminen. Vahingot kohdistuvat useimmiten omaisuuteen, mutta myös tietoihin, toimintaan ja henkilöihin. Ohjeessa ei käsitellä työsuojelua, ympäristönsuojelua eikä varautumista poikkeusoloihin.

Kouvolassa 19.12.1994

Työryhmä

Sisältö

1 YLEISTÄ

Yhteiskunnassa tapahtuneen kehityksen myötä ovat työympäristön turvallisuusriskit varsinkin viime vuosina voimakkaasti lisääntyneet. Pääosin riskit ovat olleet omaisuuteen kohdistuvia, mutta myös henkilöön kohdistuvien riskien määrä on ollut selkeässä kasvussa.

Yksityisellä sektorilla asia on tiedostettu, minkä seurauksena on luotu käsite yritysturvallisuus. Teollisuuden ja Työnantajain Keskusliiton alaisena toimiva Yritysturvallisuuden neuvottelukunta on määritellyt yritysturvallisuuden osa-alueet varsin kattavasti, mihin perustuen yritykset ovat voineet laatia yksityiskohtaiset turvallisuussuunnitelmansa.

Valtion sektorilla kaikki hallinnonalat kattava ohjaus turvallisuusriskien minimoimiseksi on toistaiseksi suuntautunut lähinnä tietoturvallisuuteen ja työsuojeluun muiden turvallisuuden osa-alueiden jäädessä vain satunnaisten virastokohtaisten ohjeiden varaan. Tästä on seurannut, että turvallisuuskysymyksiin paneudutaan riittämättömästi ja usein vasta vahingon jo tapahduttua.

Tässä ohjeessa tarkastellaan turvallisuuden keskeisillä osa-alueilla ilmeneviä turvallisuusriskejä sekä keinoja riskien minimointiin. Tietoturvallisuuden osalta tarkastelu keskittyy lähinnä atk:n käyttäjistä johtuvien riskien minimointiin, koska jo olemassaoleva ohjeistus tietoturvallisuuden alueella on muilta osiltaan varsin kattava ja lisäksi jatkuvassa kehitysprosessissa. Toimeksiannon mukaisesti tarkastelun ulkopuolelle on jätetty varautuminen poikkeusoloihin ja työsuojelu.

Lähtökohtia turvallisuusjärjestelmien rakentamiselle ovat:

* turvallisuusstrategia
* turvallisuus- ja riskianalyysi
* riskiluokitus
* turvallisuussuunnitelma.

Nämä tekijät muodostavat perustan, jolle toimivien turvallisuusjärjestelmien luominen nojaa. Vastuu toteutuksesta, ylläpidosta ja kehittämisestä koskee koko organisaatiota.

2 TURVALLISUUSSTRATEGIA

Työympäristön turvallisuusriskien torjunta edellyttää paitsi riskien tiedostamista myös taloudellisten voimavarojen käyttöä. Taloudellisista syistä jää riskien torjunta usein riittämättömäksi. Toisaalta rajattomalla taloudellisella panostuksellakaan eivät kaikki riskit ole vältettävissä. Huolellisella panos/tuotos -tarkastelulla turvallisuusjärjestelyjen taloudelliset vaikutukset voidaan optimoida työympäristön yksityiskohtaista turvallisuussuunnitelmaa laadittaessa.

Tavoitteena on omaisuuden ja tienpidon häiriöttömän toiminnan turvaaminen mahdollisimman hyvin kaikissa ennalta arvattavissa olevissa riskitilanteissa.

3 TURVALLISUUS- JA RISKIANALYYSI

Riskillä tarkoitetaan vahingonvaaraa eli mahdollisuutta tapahtumalle, joka vahingoittaa omaisuutta, toimintaa tai henkilöä ja vahingonvaaran todennäköisyys on suurempi kuin nolla.

Organisaation turvallisuusriskit jakaantuvat useille turvallisuuden eri osa-alueille, joista pääosan muodostavat:

* toimitilaturvallisuus
* tietoturvallisuus
* henkilöturvallisuus
* toimintaturvallisuus.

Osa-alueilla voi ilmetä epälukuinen määrä erityyppisiä riskejä. Sama riskityyppi voi esiintyä useammallakin kuin yhdellä turvallisuuden osa-alueella.

Riskianalyysin avulla voidaan tunnistaa riskit ja arvioida vahinkotapahtuman todennäköisyys sekä odotettavissa olevat vahingot.

Vahinkoriskit voidaan jakaa esimerkiksi seuraavasti:

* vahinkotapahtuman mukaiset riskit
* kohteen mukaiset riskit
* toiminnanmukaiset riskit
* ympäristöriskit
* erityisriskit
* muutosriskit.

Joukko vahinkotapahtuman mukaisia riskejä on lueteltu riskien tärkeysjärjestysluettelossa. (Kohta 5.6).

Kohteen mukaiset riskit jakaantuvat seuraavasti:

* henkilöriskit
* omaisuusriskit (varallisuusriskit, esineriskit).

Erityisriskejä ovat muun muassa:

* kuljetusriskit
* projektiviennin riskit
* tietotekniikka- ja tietoriskit
* keskeytysriskit
* tuoteriskit.

Muutosriskit:

* sosiaalinen kehitys
* poliittinen kehitys
* tekninen kehitys
* arvostusten muutos.

Tässä ohjeessa on keskitytty tarkastelemaan lähinnä kohteen mukaisia riskejä ja niiden torjuntaa jakamalla riskit viiteen eri tyyppiin.

4 RISKITYYPIT

4.1 Omaisuusriskit

* Anastus
* ilkivalta, sabotaasi
* huolimattomuus
* toimintavirhe
* palo, räjähdys, sortuminen
* petos, kavallus, väärinkäyttö
* luonnonilmiö
* katoaminen
* tuhoutuminen
* laite- tai konerikko.

4.2 Tietoturvallisuusriskit

* Hallinnollinen riski
* henkilöriski
* fyysinen riski
* tietoliikenneriski
* laitteistoriski
* ohjelmistoriski
* tietoaineistoriski
* käyttöriski.

4.3 Henkilöriskit

A. Henkilöön kohdistuvat riskit:

* liikenne
* vaaralliset työt
* puutteellinen siisteys ja järjestys
* vaaralliset aineet
* vaaralliset koneet ja laitteet
* melu, tärinä
* ergonomiset haittatekijät.

B. Henkilöstä johtuvat riskit:

* esiintyvät muissa riskityypeissä ja ne on käsitelty asianomaisissa kohdissa.

4.4 Toimintariskit

* Omaisuusvahingosta tai toimintavirheestä aiheutuva keskeytys
* toimintavastuu
* sopimusvastuu
* imagoriskit.

4.5 Muut riskit

* Ympäristövastuusta johtuvat riskit
* varmuus- ja valmiusvarastointiin liittyvät riskit
* ulkomaantoiminnot
* muut mahdolliset riskit, jotka on tiedostettava kunkin työympäristön turvallisuussuunnitelmaa valmisteltaessa tapauskohtaisesti.

5 RISKIT JA NIIDEN HALLINTA

Eri riskityypeissä esiintyvät yleisimmät riskien kohteet sekä keinoja riskien torjumiseksi.

5.1 Omaisuusriskit

5.1.1 Anastus

* Mikrot ja oheislaitteet ohjelmistoineen
* televisiot, videot, radiot
* videokuvauslaitteet ja valokuvauskamerat
* toimistokoneet ja -kalusto
* matkapuhelimet
* mittausvälineet
* työkalut
* varaosat ja tarvikkeet
* ajoneuvot, koneet ja lisälaitteet
* materiaalivarastot
* laiteasemat
* liikenteen mittaus- ja ohjauslaitteet
* arvopaperit ja rahatavarat
* alkuperäiset ja keskeneräiset asiakirjat (kartat, suunnitelmat ja muovit)
* alkuperäistositteet
* henkilötiedot
* tiloissa työskentelevien henkilökohtainen omaisuus.

Riskien hallinta

* Tonttien aitaus ja lukittavat portit
* ovien lukitus ja avainten valvonta
* valaistus ja hälytysjärjestelmät
* esineiden merkitseminen pysyvällä tavalla
* tärkeimpien esineiden seuranta ja luovutus kuittausta vastaan
* kulkijoiden valvonta
* omaisuuden, kuten alkuperäisasiakirjojen, keskeneräisten asiakirjojen, levykkeiden, arvopapereiden, henkilöstötietojen, tositteiden jne. säilyttäminen lukituissa tiloissa
* motivointi ja asenteiden muokkaaminen omaisuuden säilyttämiseksi ja siihen kohdistuvien vahinkojen välttämiseksi
* henkilövalinnat ja perehdyttäminen
* henkilökohtaisen vastuun lisääminen hallussa olevan omaisuuden säilyttämisestä
* siivous- ja huoltohenkilökunnan luotettavuus
* ulkopuolisten asiakkaiden tarkkailu.

5.1.2 Ilkivalta ja sabotaasiriskit

* Omaisuuden turmeleminen.

Riskien hallinta

* Ulkopuolisten pääsyn estäminen työ- ja toimistotiloihin ilman valvontaa
* työajan ulkopuolella tiloissa vierailevien henkilöiden luotettavuuden hallitseminen.

5.1.3 Huolimattomuus

* Työvälineiden ja asiakirjojen välinpitämätön käsittely ja heitteille jättäminen
* ovien lukitsematta jättäminen
* toisen hallinnassa olevien koneiden, laitteiden, asiakirjojen jne. luvaton haltuunotto ja palauttamatta jättäminen
* yhteiskäytössä olevien koneiden huolimaton käsittely
* koneen tai laitteen rikkominen ja siitä ilmoittamatta jättäminen
* leväperäinen suhtautuminen salasanoihin, ohjelmankäyttövaltuuksiin ja ulkopuolisen käyntiin omalla päätteellä
* annetaan asiaa tuntemattoman kokeilla teknisiä laitteita.

Riskien hallinta

* Neuvomalla, opastamalla, kouluttamalla ja tiedottamalla
* esimiehen valvonta
* omaisuuden käytön kontrollointi (saa vain kuittausta vastaan, löytyy vain tietystä paikasta, vain tietyt käyttäjät, salasanat, lukitukset jne.)
* jokaisella esineellä oma paikkansa
* työkoneiden säilytys maastokohteissa asutuksen läheisyydessä
* arvokkaita esineitä ei jätetä näkyville tai helposti saataville.

5.1.4 Työ- ja toimintavirhe

* Omaisuuden rikkoutuminen taitamattomuuden takia
* kokeilunhalu.

Riskien hallinta

* Koulutus, työnopastus, ohjeistus
* oikeat henkilövalinnat
* tuloskeskustelut, toimenkuvat, oikea valtuuksien ja vastuun jako.

5.1.5 Palo, räjähdys ja sortuminen

* Sähköiset laitteet
* palavat nesteet ja räjähdysaineet
* tulityöt
* poltto- ja räjähdysainevarastot
* kaasupullot
* soranottoalueet ja materiaalivarastot
* siilot.

Riskien hallinta

* Laitteiden huolto ja kunnossapito
* tiedottaminen
* huolellisuus
* sammutusvälineet kunnossa
* palotarkastukset
* räjähdysainevarastot (erillinen ohje)
* soranottoalueet ja materiaalivarastot (erillinen ohje)
* asiattomien pääsy siiloille estettävä
* henkilökunnan omatoiminen valvonta.

5.1.6 Petos, kavallus ja varastaminen

* Rahavarat
* väärinkäytökset
* valtion omaisuuden luvaton ottaminen omaan käyttöön tai myyminen omaan lukuun.

Riskien hallinta

* Oikeat henkilövalinnat
* vaarallisten työyhdistelmien syntymisen ehkäiseminen
* perehdyttäminen
* riittävät rangaistusmenetelmät, jotka ovat yleisesti tiedossa
* valvonta.

5.2 Tietoturvallisuusriskit

Valtioneuvosto on 4.2.1993 tehnyt periaatepäätöksen tietoturvallisuuden kehittämisestä valtionhallinnossa (VM 4.2.1994 nro VM 1/73/93). Päätöksen perusteella on koottu tielaitokselle sovellettu tietoturvakansio. Kansio on atk-ryhmällä sekä Kouvolassa että Mikkelissä.

Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien ja palveluiden suojaamista normaali- ja poikkeusoloissa lainsäädännön ja muiden toimien avulla. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä suojataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien tai tahallisten, tuottamuksellisten ja tapaturmaisten inhimillisten tekojen aiheuttamilta uhilta ja vahingoilta.

Tietoturvallisuus voidaan jakaa kahdeksaan osa-alueeseen seuraavasti:

1 Hallinnollinen tietoturvallisuus
2 Henkilöturvallisuus
3 Fyysinen turvallisuus
4 Tietoliikenneturvallisuus
5 Laitteistoturvallisuus
6 Ohjelmistoturvallisuus
7 Tietoaineistoturvallisuus
8 Käyttöturvallisuus.

Seuraavissa kohdissa käsitellään asioita, jotka koskevat enemmän tavallista atk:n hyväksikäyttäjää kuin ATK-ryhmää. Keskuskoneisiin ja tietoliikenteeseen liittyvät asiat, jotka koskevat vain ATK-ryhmää, löytyvät tietoturvakansiosta.

5.2.1 Hallinnollinen tietoturvallisuus

Riskit

* Tietoturvallisuuden tärkeyttä ei ole tiedostettu
* valvontajärjestelmien toimimattomuus.

Riskien hallinta

* Määritellään tietoturvavastuut ja organisaatio
* määritellään henkilövastuut, muut vastuut ja organisaatio
* kartoitetaan, luokitellaan ja luetteloidaan tietovarat
* pidetään ohjeistus ja ohjeet ajantasalla
* tietoturvallisuuskoulutus ja perehdyttäminen
* valvotaan ja tarkastetaan jatkuvasti.

5.2.2 Henkilöturvallisuus

Vaikka henkilöstö on organisaation tärkein voimavara, on se myös samalla tietoturvallisuuden suurin riskitekijä.

Riskit

* Henkilön tausta
* sopivuus tehtävään
* tehtävän päätyttyä pääsy tietoverkkoon sallittu
* henkilöllä on liian laajat käyttöoikeudet
* henkilöllä on päätösvaltaa liian monessa asiassa
* laitoksen ulkopuolisten palvelujen tuottajat (siivoojat, huoltomiehet ym.) tai vierailijat
* klikkiytyminen ja hyväuskoisuus.

Riskien hallinta

* Työhönottovaiheessa selvitetään henkilötaustat
* tehtävästä erotessa tai pitkäaikaisissa poissaoloissa avaimet ja aineistot pois, käyttöoikeudet peruttava
* vain työtehtävien edellyttämät käyttöoikeudet
* kulunvalvonta
* ulkopuolisten valvonta
* salassapitovelvollisuus
* käyttäjän oman vastuun korostaminen
* turvallisuusasioiden ja riskien tiedostaminen.

5.2.3 Fyysinen turvallisuus

* Riskit ja riskien hallinta soveltuvin osin samoin kuin kohdassa 5.1 Omaisuusriskit.

5.2.4 Tietoliikenneturvallisuus

Riskit

* Ulkopuoliset talossa tai talon ulkopuolelta pääsevät verkkoon.

Riskien hallinta

* Verkkojen salasanat pidetään vain omana tietona
* vain takaisinsoittomodemeja lähiverkkoon (tunnistus)
* tietoliikennelaitteet suojatussa paikassa.

ATK:n tekninen tuki hoitaa tai vastaa tietoliikenneturvallisuuteen liittyvistä asioista.

5.2.5 Laitteistoturvallisuus

Riskit

* Strategisten koneiden rikkoutuminen
* sähkökatkokset
* "väärää sähköä"
* huoltotoimenpiteet.

Riskien hallinta

* Varakoneet tai UPSit tärkeimmille koneille (serverit, tiesääkeskuskone)
* huollot ja huoltosopimukset atk-ryhmän kautta
* koneiden vaihto ja asennus ammattihenkilöiden toimesta
* koneet vain ATK-käyttömerkillä varustettuihin maadoitettuihin pistorasioihin (laskukoneet, radiot, kahvinkeittimet yms. muihin pistorasioihin).

5.2.6 Ohjelmistoturvallisuus

Riskit

* Levykkeitä ei ole virustarkastettu (tai tietoliikenneyhteyksien kautta siirretyt ulkopuoliset tiedostot)
* laittomat levykkeet
* laitevarkauksien yhteydessä ohjelmistot ja datat menevät mukana
* ohjelmistojen laiton levitys
* uusien ohjelmien rakennusaikataulu
* ohjelmistosopimukset
* asiaankuulumattomat pääsevät ohjelmistoon käsiksi
* ohjelmien sisältämiä tietoja ei ole suojattu
* ohjelmakontrollit puuttuvat
* dokumentointi ei ole ajantasalla ja käytössä

Riskien hallinta

* Kaikki talon ulkopuolelta tulevat disketit on virustarkastettava
* ostettava ohjelmistojen viralliset versiot
* data-tiedoista on ainakin varmistukset oltava levykkeillä, nauhoilla yms. varmassa tallessa
* ATK-ryhmä huolehtii keskitetysti alkuperäisistä ohjelmistolevykkeista ja ohjelmien ylläpitämisestä
* käyttöoikeudet vain todellisille tarvitsijoille
* tietoliikenneohjelmistoissa tarkka vastapuolen tarkistus
* luotettavat toimittajat
* ilmoitus koneen oudosta käyttäytymisestä
* ATK-ryhmä asentaa ohjelmat tai on ainakin mukana
* yksikössä kehitetyt ohjelmat dokumentoitava
* mikro- ja keskuskoneiden ohjelmien rekisteröinti ja käyttöoikeudet
* lokitiedostot tapahtumista
* salasanat
* mikroserverin suojaukset.

5.2.7 Tietoaineistoturvallisuus

Riskit

* Käyttäjä saa tietoja, jotka eivät hänelle kuulu
* syöttödokumenttien arkistointiaika
* kirjausketjun puuttuminen ja tietojen säilyttäminen vain tiedostoissa.

Riskien hallinta

* Asiakirjajulkisuus
* arkistojulkisuus
* tietosuoja
* luottamuksellisten tietojen säilytys
* tulosteiden tuhoaminen
* suojakopiot (muualla, poikkeustilanne).

5.2.8 Käyttöturvallisuus

Tietojen käsittelyssä on merkittävä osuus siirtynyt mikroille. Mikroilla tehdään nykyään asioita, joita joku vuosi sitten tehtiin keskuskoneympäristössä. Keskuskoneissa on kehittyneet välineet tietoturvallisuudesta huolehtimiseen, mutta mikroista sen kaltaiset ominaisuudet puuttuvat lähes kokonaan. Mikrojen käyttöä ei voida myöskään valvoa kuten keskuskoneympäristössä, joten vastuu turvallisesta työskentelystä jää käyttäjille.

Riskit

* Ei osata käyttää mikroa turvallisuuden kannalta oikein (säännölliset varmistukset, keskeneräisten töiden tallennukset, virustarkastukset, salasanojen vaihdot jne.)
* epämääräiset toipumissuunnitelmat (keskuskoneet, serverit)
* vaaralliset työyhdistelmät (esim. kassa ja kirjanpito)
* vain yksi hallitsee koneen, järjestelmän, asian...
* liian laajat käyttöoikeudet järjestelmissä
* data-tiedostoja ei ole varmistettu
* salasanat näkyvillä tai helposti saatavilla
* huoneessa mikro auki (yhteys verkkoon, ohjelmaan tai järjestelmään) eikä työntekijä ole paikalla
* aikataulut pettävät (lähinnä keskuskonejärjestelmät)
* kuppikuntaisuus.

Riskien hallinta

* Käyttäjän on asennoiduttava tietoturvallisuuteen vakavasti
* käyttäjien koulutus
* selvät toipumisdokumentit
* ATK-ryhmä hoitaa säännöllisesti keskustietokone- ja serverivarmistukset
* käyttäjät hoitavat omien mikrojensa varmistukset
* varmistusohjeet
* salasanat piiloon ja vaihdetaan tietyin väliajoin
* huoneesta poistuttaessa vähänkin pitemmäksi aikaa on huoneen ovi lukittava tai ainakin katkaistava yhteys verkkoon, ohjelmaan tai järjestelmään
* käyttöoikeuksien määrittely
* pääkäyttäjät/operaattorit pitävät aikatauluista kiinni
* yhteistyö
* keskeneräisten töiden tallennus.

5.3 Henkilöriskit

5.3.1 Henkilöön kohdistuvat riskit

* Kuuluvat työsuojelun piiriin. Erilliset ohjeet annettu.

5.3.2 Henkilöstä johtuvat riskit

* Esiintyvät muissa riskityypeissä ja niitä on käsitelty asianomaisissa kohdissa.

5.4 Toimintariskit

5.4.1 Omaisuusvahingosta tai toimintavirheestä johtuvat toiminnan keskeytykset

* Henkilöominaisuudet ja ammattitaidon puute
* koneiden ja laitteiden huollon tai kunnostuksen laiminlyönti
* sijaisuusjärjestelyjen ja varajärjestelmien puuttuminen tai heikkous
* tietämättömyys miten vahingon sattuessa pitää toimia ja tiedottaa
* johtamisen heikkous
* työkuormitus.

Riskien hallinta

* Varajärjestelmien ja sijaisuuksien luominen ja niiden ajoittainen toimivuuden testaus
* koneiden ja laitteiden huollon varmistaminen ja sen toimivuus
* varmistaminen, että henkilöllä on riittävä ammattitaito ja tieto koneiden ja laitteiden hallitsemisessa
* ylläpidettävä valmius 'vastata' omaisuus- ja toimintariskeihin
* henkilöstön fyysisestä ja henkisestä hyvinvoinnista huolehtiminen.

5.4.2 Toimintavastuusta johtuvat riskit

* Heikko työmoraali ja piittaamattomuus ohjeista
* henkilöstövalintojen heikkous ja riittämätön ammattitaito
* työn ja vastuunjaon puuttuminen tai sen heikkous; esimerkiksi vastuu ja osaaminen eivät kohtaa toisiaan
* johtamisen heikkous tai puute
* henkilön työkyvyn äkillinen heikkeneminen ja pitkät poissaolot
* yhteistyökyvyttömyys.

Riskien hallinta

* Henkilöiden sijoittumista oikeisiin tehtäviin edistetään haastattelemalla, testaamalla ja tekemällä halukkuuskyselyjä
* kehittämällä johtamistapaa
* työn- ja vastuunjako nähtävä oikeassa suhteessa henkilön osaamiseen nähden
* henkilökunnan ammattitaidon ylläpitäminen ja kehittäminen
* yhteistyön arvostaminen työyhteisössä ja sen kehittäminen.

5.4.3 Sopimusvastuusta johtuvat riskit

* Sovittujen toimintamallien, vastuun ja vallankäytön laiminlyöminen
* valvonnan puute
* suulliset sopimukset (lupausten rikkominen)
* toistuvat laiminlyönnit (heikentävät uskottavuutta ja toimintakykyä sekä vaikuttavat negatiivisesti yrityskuvaan)
* sopimusten vähättely ja oman minäkuvan korostaminen.

Riskien hallinta

* Ohjeistus ajantasalla ja ohjeiden noudattaminen
* käytetään asiantuntijoita
* pidetään sovitusta toiminta- ja vastuunjaosta kiinni
* hyvän yrityskuvan ylläpitäminen
* työjärjestyksen ylläpitäminen
* laatu ja prosessikuvaukset kunnossa
* kirjalliset sopimukset.

5.5 Muut riskit

5.5.1 Ympäristövastuusta johtuvat riskit

* Piirin ympäristönhoidon periaatteet 1994 - 1996 -julkaisu; hyväksytty 30.5.1994.

5.5.2 Varmuus- ja valmiusvarastot

Varmuusvarastoilla turvataan kriisi- ja normaaliajan toiminta.

* Ulkopuolisten aiheuttamat vahingot ja hävikki.

Riskien hallinta

* Katso kohta 5.1 Omaisuusriskien hallinta.

5.5.3 Ulkomaantoiminnot

* Terveysriskit
* lainsäädäntö
* matkustaminen
* rikollisuus
* toimintatavat, kulttuuri, käyttäytyminen
* kielivaikeudet
* rahaliikenne, tullit.

Riskien hallinta

* Tiedotus, opastus, koulutus
* tarpeelliset paperit kunnossa
* rokotukset kunnossa
* kulttuurin tuntemus.

5.6 Riskien tärkeysjärjestys

Riskit luokitellaan tärkeysjärjestykseen niiden todennäköisyyden ja suurimman vahingon perusteella. Kumpikin tekijä arvioidaan asteikolla 0 - 5. Saatujen lukujen (kertoimien) tulo, ns. riskitulo, kuvaa riskin suuruutta. Riskinhallintatoimet kohdistetaan suurimpiin riskeihin suurimmasta alkaen. Kaikki toimet suhteutetaan riskin suuruuteen siten, että riskinhallinnasta syntyvät kustannukset jäävät pienemmiksi kuin riskin suuruus. Luokittelussa voi käyttää riskien tärkeysjärjestystaulukkoa, jota voi täydentää tapauskohtaisesti.

Riski	Todennäköisyys (0-5)	Vahingon suuruus max (0-5)	Riskitulo (0-25)
Anastus			
Avainhenkilön ero			
Hukka			
Huolimattomuus			
Häviäminen			
Ideavarkaus			
Ilkivalta			
Katoaminen			
Kavallus			
Keskeytys			
Konerikko			
Kuljetusvahinko			
Kurittomuus			
Liikenneonnettomuus			
Luonnonilmiö			
Lämpötilan muutos			
Magneettinen pulssi			
Materiaalivika			
Murto			
Nestevahinko			
Petos			
Pomminuhka			
Rikkoontuminen			
Ryöstö			
Räjähdys			
Sabotaasi			
Sairaus			
Sortuma			
Sähköilmiö			
Sähkökatko			
Tapaturma			
Tiedostovarkaus			
Tietovuoto			
Toimintavirhe			
Tuhoutuminen			
Tulipalo			
Työvirhe			
Vaaralliset aineet			
Valtaus			
Vammautuminen			
Varkaus			
Väärinkäyttö			
Ydinvaara			
Ympäristön uhka			

6 TURVALLISUUSSUUNNITELMAT

Työympäristössä esiintyvien riskien laatu ja laajuus on riippuvainen harjoitettavan toiminnan laadusta. Siksi on perusteltua kartoittaa riskitekijät työympäristökohtaisesti ja laatia suunnitelma, jota noudattaen toiminta ja omaisuus tulevat mahdollisimman hyvin turvatuiksi. Tiepiirissä suunnitelma laaditaan

* **piiri- ja maakuntakonttorille**
* **tiemestaripiireille, rakennustyömaille ja muille kiinteille hankkeille**
* **liikkuville hankkeille** (suunnitteluhankkeet, murskaus- ja päällystystyöt, ajoratamerkintätyöt, siltojen korjaus- ja rakennustyöt).

Tässä ohjeessa on esitetty yleisimpiä riskityyppejä sekä keinoja tarkoituksella helpottaa suunnitelmien laatimistyötä. Riskit ja niiden torjuntakeinot ovat kuitenkin aina työympäristökohtaisia, mikä on tärkeää muistaa suunnitelmaa laadittaessa.

Hankkeen päällikkö vastaa hanketason turvallisuussuunnitelman laatimisesta ja ylläpidosta.

Tiejohtaja nimeää piirikonttorin ja maakuntakonttorin turvallisuussuunnittelun vastuuhenkilön.

Kiinteistöpäällikkö ohjaa ja valvoo piiritasolla turvallisuusasioita.

ESIMERKKEJÄ KÄYTÄNNÖN RATKAISUISTA ERÄISSÄ TAPAUKSISSA

Elektroniset hälytysjärjestelmät

Soveltuvat kiinteisiin toimipaikkoihin. Hälytys ohjautuu vartiointiliikkeeseen tai muuhun sellaiseen paikkaan, jossa on ympärivuorokautinen päivystys (ei kuitenkaan poliisille eikä aluehälytyskeskukseen). Järjestelmän rakentamiskustannukset esimerkiksi tiemestaripiirin tukikohtaan ovat noin 12 000 mk (5 kpl infrapunailmaisimia, hälytys vartiointiliikkeeseen, joka perii hälytyksen vastaanottovalmiudesta 300 mk/kk).

Kameravalvonta

Soveltuu kiinteissä toimipaikoissa reaaliaikaiseen kulunvalvontaan asiakas- ja työtiloissa (esim. piirikonttori). Videonauhurilla varustettuna ja yhdistettynä elektroniseen hälytysjärjestelmään tallentaa tapahtumat hälytyksen alkamishetkestä lukien.

Kustannukset ovat merkittävästi riippuvaisia järjestelmään kytkettyjen kameroiden lukumäärästä.

Valo- ja/tai äänihälytin

Soveltuu erityisesti liikkuvien työkohteiden omaisuuden suojeluun edellyttäen, että kyseinen omaisuus on jätetty asutulle alueelle (hälytys voitava havainnoida). Kustannukset ovat 2 000 - 3 000 mk/hälytinyksikkö.

Tässä yhteydessä todettakoon, että liikkuvien työkohteiden omaisuus (koneet, ajoneuvot, laitteet yms.) tulisi aina sijoittaa työajan ulkopuoliseksi ajaksi paikkaan, jossa se olisi sovitusti silmälläpidon alaisena.

Tiedon turvaaminen

Päivittäinen toiminta eri työympäristöissä perustuu yhä enenevässä määrin tietotekniikan hyväksikäyttöön, joten anastuksen tai ilkivallan kohteena on usein myös tietojenkäsittelylaitteisto. Omaisuusvahinkotapauksissa menetetyn laitteiston arvo on kuitenkin usein vain murto-osa samassa yhteydessä laitteiston mukana menetetyn tiedon arvosta. Tiedon säilyttämisestä varmuuskopioiden avulla onkin huolehdittava erityisesti sijainniltaan sellaisessa työmympäristössä, jossa olot anastukselle ja ilkivallalle ovat suotuisat (syrjäinen sijainti, ei valoa, ei liikennettä).

Tietoja turvajärjestelmiin liittyvistä kysymyksistä antavat paikalliset turvallisuusalan liikkeet sekä piirin sähköteknikot.

TIEL KaS 10/94